**UNITED STATES DISTRICT COURT**
**FOR THE SOUTHERN DISTRICT OF TEXAS**
**HOUSTON DIVISION**

| | |
|---|---|
| **IN RE FRANCESCA'S ACQUISITION, LLC DATA SECURITY BREACH LITIGATION** | Lead Case No. 4:23-cv-03881<br><br>Consolidated Case:<br><br>4:23-cv-04049 |

# CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Taylor Doherty, Alessandra Jimenez, Kayla Stewart, Ellie Bley, and Wendy Nolasco, on behalf of themselves and all others similarly situated, bring this Consolidated Class Action Complaint ("Complaint") against Defendants Francesca's Acquisition, LLC, Tiger Capital Group, LLC, and SB360 Capital Partners, LLC ("Francesca's" or collectively, "Defendants") and allege, upon personal knowledge as to their own actions and their counsel's investigation, including review of public documents, and upon information and belief as to all other matters, as follows:

## NATURE OF THE CASE

1. Plaintiffs bring this class action against Francesca's for its failure to properly secure and safeguard personally identifiable information ("PII" or "Private Information") of Plaintiffs and other similarly situated current and former employees and customers (collectively, the "Class Members") from hackers. Defendants failed to provide timely, adequate, and accurate notice to victims that the integrity of their PII had been compromised and stolen. Plaintiffs' and Class Members' compromised PII included their first and last names, Social Security numbers, and financial account information belonging to roughly 58,387 Class Members.[1]

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/ff7c9ad6-019a-4bf8-a852-0e5c80c70c76.shtml (last accessed Jan. 31, 2024)

2. Francesca's is a women's fashion boutique founded in 1999 that sells fashion apparel, jewelry, accessories, and gifts. It has more than 450 stores across 45 states and, upon information and belief, an annual revenue of $407 million. Francesca's was sold to Francesca's Acquisition, LLC in 2021.

3. On or around January 31, 2023, Francesca's discovered a data security incident through which an unauthorized third party accessed Francesca's network and files in its computer systems, with such access having taken place from January 12 through January 31, 2023 (the "Data Breach"). Consequently, Plaintiffs' and Class Members' PII was compromised, including their first and last names, Social Security numbers, and their financial account information.

4. Upon discovery of the Data Breach, Francesca's initiated an investigation with the aid of third-party data security specialists. This investigation, which concluded on August 8, 2023, determined that Private Information belonging to Francesca's customers and employees had been stolen by cybercriminals in the successful attack.

5. Despite the breadth and sensitivity of the PII exposed, and the attendant consequences to Plaintiffs and Class Members as a result of the exposure, Francesca's failed to disclose the Data Breach for ***approximately eight months*** from the time the Data Breach occurred, on or about September 25, 2023, further exacerbating harm to Plaintiffs and the Class.

6. This Data Breach was a direct result of Francesca's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect Plaintiffs' and Class Members' PII.

7. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government

benefits and/or medical services, filing fraudulent tax returns using Class Members' information, and giving false information to police during an arrest.

8. Francesca's disregarded the rights of Plaintiffs and Class Members by: intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiffs' and Class Members' PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to monitor and timely detect the Data Breach; failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach; and failing to provide comprehensive and effective credit protection services after notification of the Data Breach.

9. As a result of Francesca's failure to implement and follow basic security procedures, the PII of past and current employees, as well as customers, of Francesca's is now in the hands of thieves who, upon information and belief, have committed criminal acts against Plaintiffs and the Class by misusing their data and/or have published and/or sold their data on the internet (i.e., the "dark web") for others to view, access, and/or misuse. Plaintiffs and Class Members have had to spend, and will continue to spend, significant amounts of time and money to protect themselves from the adverse ramifications of the Data Breach and will forever be at a heightened risk of identity theft and financial fraud.

10. There has been no assurance offered by Francesca's that all personal data or copies of data have been recovered or destroyed, or that it has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

11. Therefore, Plaintiffs and Class Members are at an imminent, immediate, and continuing increased risk of suffering ascertainable losses in the form of identity theft and other fraudulent misuse of their Private Information, out-of-pocket expenses incurred to remedy or mitigate

the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

12. Plaintiffs bring this action to address Defendants' inadequate safeguarding of their and Class Members' PII that it collected and maintained, and its failure to provide timely and adequate notice to Plaintiffs and Class Members of the types of information accessed, and that such information was subject to unauthorized access by cybercriminals.

13. As a result of Francesca's failure to adequately satisfy its contractual, statutory, and common law obligations, Plaintiffs and Class members suffered injuries including, but not limited to:

- The actual fraudulent misuse of their Private Information;
- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges;
- Time needed to change usernames and passwords on their accounts;
- Time needed to investigate, correct and resolve unauthorized access to their accounts;
- Time needed to deal with spam messages and e-mails received subsequent to the Data Breach; and
- Charges and fees associated with fraudulent charges on their accounts; and the continued and increased risk of compromise to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect their Private Information.

14. Plaintiffs seek to remedy these harms on behalf of themselves and all others similarly situated whose Private Information was compromised as a result of the Data Breach.

15. Accordingly, Plaintiffs, on behalf of themselves and the Class, assert claims for negligence, negligence *per se*, invasion of privacy, breach of implied contract, unjust enrichment, violations of the California Constitution, the California Consumer Privacy Act, the California Consumer Legal Remedies Act, the California Unfair Competition Law, and the California Consumer Records Act, and for declaratory/injunctive relief.

## PARTIES

16. Plaintiff Taylor Doherty is an individual citizen of the State of Massachusetts.

17. Plaintiff Alessandra Jimenez is an individual citizen of the State of Illinois.

18. Plaintiff Kayla Stewart is an individual citizen of the State of Maryland.

19. Plaintiff Ellie Bley is an individual citizen of the State of Pennsylvania.

20. Plaintiff Wendy Nolasco is an individual citizen of the State of California.

21. Defendant Francesca's Acquisition, LLC is a limited liability company organized under the laws of Delaware with its principal place of business located at 8760 Clay Road in Houston, Harris County, Texas.

22. Defendants Tiger Capital Group and SB360 Capital Partners, LLC each have an ownership interest in Francesca's Acquisition, LLC and remain active in its operations.

23. Defendant Tiger Capital Group, LLC is a limited liability corporation organized under the laws of Massachusetts with its principal place of business located at 60 State Street, Floor 11, No. 50, Boston, Massachusetts.

24. Defendant SB360 Capital Partners, LLC is a limited liability corporation organized under the laws of Delaware with its principal place of business located at 4300 E. 5th Avenue, Columbus, Ohio.

## JURISDICTION AND VENUE

25. Pursuant to the Court's Order for Conference and Disclosure of Interested Parties dated October 16, 2023 (Doc. 3), Plaintiffs must assert diversity jurisdiction against an LLC as follows: "The citizenship of limited liability entities is determined by the citizenship of their members. *Harvey v. Grey Wolf Drilling Co.,* 542 F.3d 1077, 1080 (5th Cir. 2008). When members of a limited liability entity are themselves entities or associations, citizenship must be traced through however many layers of members there are until arriving at the entity that is not a limited liability entity and identifying its citizenship status." Despite Plaintiffs' efforts to secure this information from Francesca's Acquisition, LLC, Tiger Capital Group, LLC, and SB360 Capital Partners, LLC, each entity has failed to fully disclose its LLC members' citizenship. For example, Defendant SB360 recently advised Plaintiffs that it is "unwilling to provide any additional information regarding the ownership structure . . . 'without a court order[.]'" *See* Conor Hafertepe Email to Tyler Bean, attached hereto as **Exhibit 1**. Plaintiffs thus request the Court order such information be provided to Plaintiffs immediately.

26. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Francesca's. Thus, minimal diversity exists under 28. U.S.C. § 1332(d)(2)(A). This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

27. This Court has personal jurisdiction over Francesca's because Francesca's headquarters and principal place of business is located in the Houston Division of the Southern District of Texas.

28. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Francesca's headquarters and principal place of business is in the Houston Division of the Southern District of Texas.

## FACTUAL ALLEGATIONS

### A. Defendants' Business and Collection of Plaintiffs' and Class Members' Private Information

29. Francesca's sells fashion apparel, jewelry, accessories, and gifts through its 457 boutiques in 45 states and, upon information and belief, generates an annual revenue of $407 million. In 2021, Francesca's was sold to Defendant Francesca's Acquisition, LLC.

30. Francesca's Holdings Corporation (and subsidiaries) were the predecessor entities of the Francesca's brand but filed for bankruptcy in December 2020. In January 2021, assets were purchased by Francesca's Acquisition LLC, Tiger Capital Group LLC, and SB360 Capital Partners, LLC. Pursuant to the sale and by operation of law, Defendants acquired the Private Information of Francesca's Holdings Corporation (and subsidiaries), as well as all legal obligations attached to the Private Information.

31. As a condition of employment with, and/or in order to make purchases from, Francesca's, Defendants have required its employees and customers to entrust them with highly sensitive personal information. In the ordinary course of employment with, and/or making purchases from, Francesca's, Plaintiffs and Class Members were required to provide Francesca's with their Private Information, including but not limited to: full names, addresses, Social Security numbers, dates of birth, driver's license numbers, financial account information including credit and debit card numbers along with security and access codes and PINs.

32. Recognizing the high sensitivity and private nature of the PII Francesca's acquires and stores with respect to its customers and employees, Francesca's, upon information and belief, promises to: keep Private Information private; comply with industry standards related to data security and the maintenance of its current and former employees' and customers' Private Information; inform them of its legal duties relating to data security and compliance with all federal and state laws protecting

customer and employee Private Information; only use and release customers' and employees' Private Information for reasons that relate to the services it provides; not store former customer or employee Private Information for longer than is necessary to carry out its business operations; and provide adequate notice to its current and former employees and customers if their Private Information is disclosed without authorization.

33. By obtaining, collecting, using, and deriving a benefit from the Class Members' Private Information, Francesca's assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Private Information from unauthorized disclosure and exfiltration.

34. Plaintiffs and Class Members relied on Francesca's to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Private Information, which Defendants ultimately failed to do. This failure resulted in cybercriminals accessing the Private Information of Francesca's current and former employees and customers.

### B. The Data Breach and Defendants' Inadequate Notice to Plaintiffs and Class Members

35. Francesca's notified all impacted current and former Francesca's employees and customers of the Data Breach on or around September 25, 2023 (the "Notice"). Defendants reported that the Data Breach occurred approximately *eight months* earlier, over the period between January 12, 2023 through January 31, 2023, and that it did not learn of the extent of the Data Breach until August 8, 2023. Francesca's' investigation of the Data Breach revealed that an "unauthorized party" gained access to its systems and ultimately accessed copies of Plaintiffs' and Class Members' Private Information. It is clear, in light of the fraudulent misuse of the stolen Private Information that has already occurred, that the data thieves carried out the Data Breach in order to either use the Private Information themselves for nefarious purposes, or to sell it on the dark web for financial gain.

36. Thus, through the Data Breach, the unauthorized cybercriminals accessed and exfiltrated a cache of highly sensitive Private Information, including Francesca's' current and former employees' and customers' first and last names, Social Security numbers, and financial information.

37. Francesca's had obligations created by contract, industry standards, and common law to keep Plaintiffs' and Class Members' Private Information confidential and protected from unauthorized access and disclosure.

38. Plaintiffs and Class Members provided their Private Information to Francesca's with the reasonable expectation and mutual understanding that Francesca's would comply with its obligations to keep such Private Information confidential and secure from unauthorized access and disclosure, and to provide timely notice of any security breaches.

39. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks carried out against employers and retailers in recent years.

40. Francesca's knew or should have known that its electronic records would be targeted by cybercriminals, yet it failed to take the necessary precautions to protect Plaintiffs' and Class Members' Private Information from being compromised.

41. In response to its admitted failure to safeguard Plaintiffs' and Class Members' Private Information, which affected at least 58,387 individuals, Defendants' purported remedy is woefully inadequate. Despite many years of future risk and exposure, Defendants' Notice only offered 12 months of credit monitoring, which is plainly insufficient under the circumstances.

### C. Francesca's Failed to Comply with FTC Guidelines

42. Francesca's was prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair

practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

43. The FTC promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

44. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[2] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[3]

45. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

46. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or

[2] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[3] *Id.*

practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

47. As evidenced by the Data Breach, Francesca's failed to properly implement basic data security practices.

48. Francesca's' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' PII evidences its negligent failure to comply with the standards set forth by Section 5 of the FTC Act, and constitute an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

49. Francesca's was at all times fully aware of the obligation to protect the PII of its current and former employees and customers. Francesca's was also aware of the significant repercussions that would result from its failure to do so.

**D. Francesca's Failed to Comply with Industry Standards**

50. As shown above, experts studying cyber security routinely identify retailers as being particularly vulnerable to cyberattacks because of the value of the PII which they collect from customers and employees and maintain in their networks.

51. Several best practices have been identified that at a minimum should be implemented by retailers like Francesca's, including but not limited to educating all employees regarding cybersecurity matters; implementing strong passwords; implementing multi-layer security, including firewalls, anti-virus, and anti-malware software; utilizing encryption, making data unreadable without a key; requiring multi-factor authentication; backing up data; and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendants failed to follow at least some, or perhaps all of, these industry best practices.

52. Other best cybersecurity practices that are standard in the retail industry include installing appropriate malware detection software; monitoring and limiting the network ports;

protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protecting physical security systems; and training staff regarding these critical points. As evidenced by the Data Breach, Defendants failed to follow these cybersecurity best practices.

53. Upon information and belief, Defendants also failed to meet the minimum standards of one or more, if not all, of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

54. These foregoing frameworks are existing and applicable industry standards in the retail industry, and Francesca's failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

### E. Francesca's Breached its Duty to Safeguard Plaintiffs' and Class Members' PII

55. In addition to its obligations under federal and state laws, Francesca's owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Francesca's owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Plaintiffs and Class Members.

56. Francesca's owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including

adequately training its employees and others who accessed PII within its computer systems on how to adequately protect PII.

57. Francesca's owed a duty to Plaintiffs and Class Members to implement processes that would detect a compromise of PII in a timely manner.

58. Francesca's owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

59. Francesca's owed a duty to Plaintiffs and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

60. Francesca's owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

61. Francesca's owed a legal duty to secure current and former employees' and customers' PII and to timely notify them of a data breach.

62. Francesca's breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Francesca's' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect current and former employee and customer PII;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to detect unauthorized ingress into its systems;

f. Failing to implement and monitor reasonable network segmentation to detect unauthorized travel within its systems, including to and from areas containing the most sensitive data;

g. Failing to detect unauthorized exfiltration of the most sensitive data on its systems;

h. Failing to train its employees in the proper handling of emails containing PII and maintain adequate email security practices;

i. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

j. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

k. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

l. Failing to adhere to industry standards for cybersecurity as discussed above; and

m. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

63. Francesca's negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' PII by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted PII.

64. Had Francesca's remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Francesca's could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential PII.

65. However, due to Defendants' failures, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and the Class Members also lost the benefit of the bargain they made with Francesca's.

### F. Francesca's Knew or Should Have Known that Criminals Target PII to Carry Out Fraud and Identity Theft

66. The FTC hosted a workshop to discuss "informational injuries," which are injuries suffered as a result of privacy and security incidents such as data breaches or unauthorized disclosure of data, injuries that Plaintiffs and Class Members were exposed to as a result of the Data Breach.[4] Exposure of highly sensitive personal information that individuals keep private may cause harm to them, such as the ability to obtain or keep employment. Individuals' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

67. Francesca's' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the retail industry and other industries holding significant amounts of PII preceding the date of the breach.

68. At all relevant times, Francesca's knew, or should have known, its former and current employees', customers', Plaintiffs', and all other Class Members' PII was a target for malicious actors. Despite such knowledge, Francesca's failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class Members' PII from cyber-attacks that Francesca's should have anticipated and guarded against.

69. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the PII of Plaintiffs and Class Members.

[4] FTC Information Injury Workshop, BE and BCP Staff Perspective, Federal Trade Commission, (October 2018), available at https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf.

70. PII is a valuable property right.[5] The value of PII as a commodity is measurable.[6] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[7] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[8] Private Information is so valuable to identity thieves that once Private Information has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

71. As a result of its real value and recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

72. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data." This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[9]

---

[5] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible...").

[6] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

[7] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[8] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[9] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last accessed November 29, 2022).

73. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[10]

74. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

75. Indeed, cyberattacks against the retail industry have been common for over ten years with the Federal Bureau of Investigation ("FBI") warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[11]

76. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[12]

77. Francesca's should have known about its data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the PII stored in its unprotected files.

---

[10] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1.

[11] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

[12] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-.warn-of-targeted-ransomware.

### G. Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

78. Cyberattacks and data breaches at retail companies like Francesca's are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

79. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[13]

80. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

[13] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf.

81. Theft of PII is serious. The FTC warns consumers that identity thieves use Private Information to exhaust financial accounts, start new utility accounts, and incur charges and credit in a person's name.

82. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[14]

83. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.

84. Identity thieves can also use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, and/or rent a house or receive medical services in the victim's name.

[14] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Jan. 19, 2022).

85. Moreover, theft of PII is also gravely serious because Private Information is an extremely valuable property right.[15]

86. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States. For example, with the PII stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members.

87. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

88. There is a strong probability that entire batches of stolen information have been dumped on the black market or are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

89. For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.

90. Cybercriminals may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information

[15] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

> may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[16]

91. Social Security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number**: *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refund, employment—even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[17]

92. For instance, with a stolen Social Security number, which is only one subset of the Private Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[18]

93. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[19] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[20] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

---

[16] *Data Breaches are Frequent*, *supra* note 11.
[17] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (emphasis added).
[18] *Id.*
[19] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (Jan. 19, 2022).
[20] *Id.* at 4

94. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[21]

95. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against companies like Francesca's is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

96. Indeed, a Social Security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[22] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[23]

97. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to PII, they *will use it*.[24]

98. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[25]

---

[21] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[22] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017, https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

[23] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[24] *Id.*

[25] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last visited Aug. 2, 2022).

99. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the victim has suffered the harm.

100. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[26]

101. Cybercriminals can post stolen PII on the cyber black-market for years following a data breach, thereby making such information publicly available.

102. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened.[27] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[28]

103. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[29]

104. It is within this context that Plaintiffs and Class Members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the

---

[26] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019, 3:39 PM), https://time.com/5643643/capital-one-equifax-data-breach-social-security/

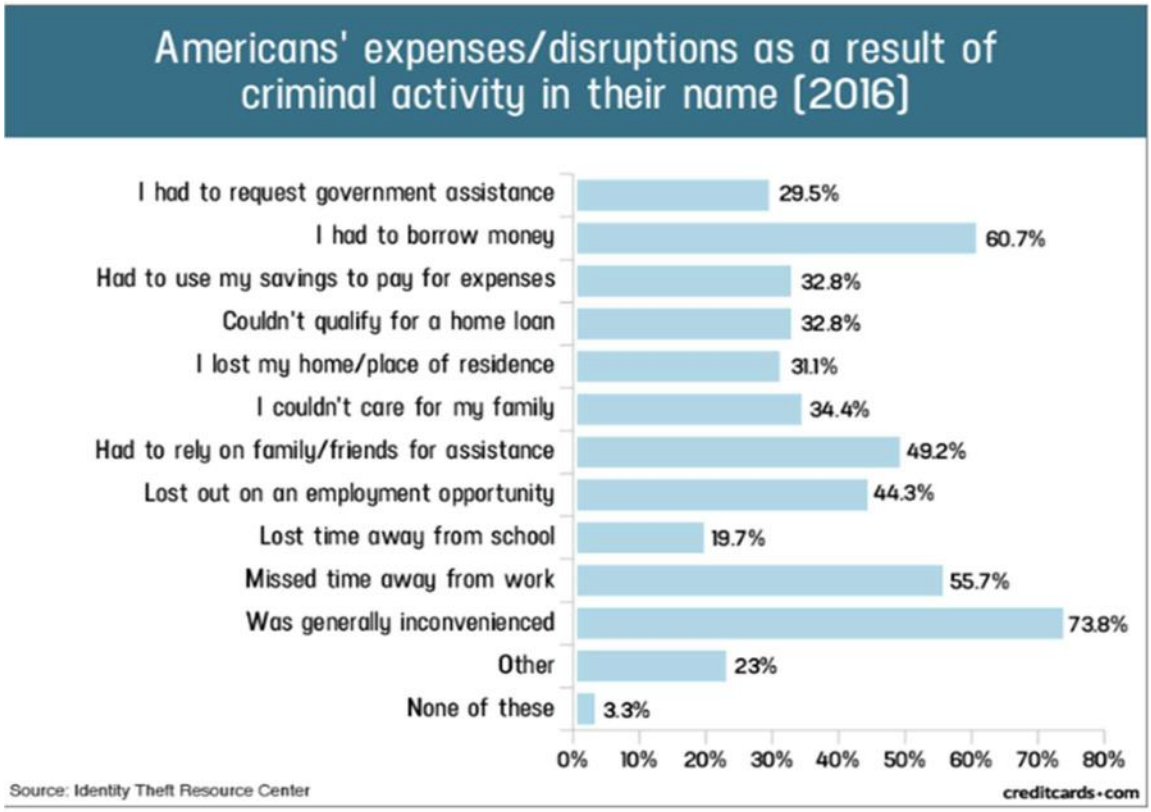
[27] *See* Medical ID Theft Checklist, *available at:* https://www.identityforce.com/blog/medical-id-theft-checklist-2.

[28] Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages")*, *available at:* https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

[29] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

information for any number of improper purposes and scams, including making the information available for sale on the black market.

105. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information.




106. Victims of the Data Breach, like Plaintiffs and Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[30]

107. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have had their PII exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs and Class

[30] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

Members must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

108. Plaintiffs and Class Members have suffered or will suffer actual harms for which they are entitled to compensation, including but not limited to the following:

a. Actual identity theft, including fraudulent credit inquiries and cards being opened in their names;

b. Trespass, damage to, and theft of their personal property, including PII;

c. Improper disclosure of their PII;

d. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their PII being in the hands of criminals and having already been misused;

e. The imminent and certainly impending risk of having their confidential Private Information used against them by spam callers to defraud them;

f. Damages flowing from Defendants' untimely (and in some cases, non-existent) and inadequate notification of the Data Breach;

g. Loss of privacy suffered as a result of the Data Breach;

h. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

i. Ascertainable losses in the form of deprivation of the value of Plaintiffs' and Class Members' Private Information for which there is a well-established and quantifiable national and international market;

j. The loss of use of and access to their credit, accounts, and/or funds;

k. Damage to their credit due to fraudulent use of their PII; and

l. Increased cost of borrowing, insurance, deposits, and other items which are adversely affected by a reduced credit score.

109. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PII, which remains in the possession of Francesca's, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Francesca's has shown itself to be wholly incapable of protecting Plaintiffs' and Class Members' PII.

110. Plaintiffs and Class Members also have an interest in ensuring that their personal information that was provided to Francesca's is removed from Defendants' unencrypted files.

111. Francesca's itself acknowledged the harm caused by the Data Breach because it offered Plaintiffs and Class Members the inadequate 12 months of identity theft protection and credit monitoring services. This limited identity theft monitoring is, however, inadequate to protect Plaintiffs and Class Members from a lifetime of identity theft risk.

112. Francesca's further acknowledged, in its letter to Plaintiffs and other Class Members, that, in response to the Data Breach, Francesca's "implemented additional technical safeguards to further enhance the security of information in our possession."

113. The Notice Letter further acknowledged that the Data Breach would cause inconvenience to affected individuals by providing numerous "steps" for Class Members to take in an attempt to mitigate the harm caused by the Data Breach, and that financial harm would likely occur,

stating: "We recommend that you remain vigilant against incidents of identity theft and fraud by regularly reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company. You can also activate the complimentary identity monitoring as described below, and you can review the enclosed 'Steps You Can Take to Help Protect Your Information' for additional resources."

114. At Defendants' suggestion, Plaintiffs and Class Members are trying to mitigate the damage that Francesca's has caused them. Given the kind of PII Francesca's made accessible to hackers, however, Plaintiffs and Class Members are certain to incur additional damages. Because identity thieves have their PII, Plaintiffs and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[31] None of this should have happened.

115. Because of the value of its collected and stored data, the retail industry has experienced disproportionally higher numbers of data theft events than other industries. For this reason, Francesca's knew or should have known about these dangers and strengthened its data security accordingly. Francesca's was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

### H. The Data Breach Was Foreseeable and Preventable

116. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of

[31] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

the biggest cybersecurity breaches: Target,[32] Yahoo,[33] Marriott International,[34] Chipotle, Chili's, Arby's,[35] and others.[36]

117. Francesca's should certainly have been aware, and indeed was aware, that it was at risk for a data breach that could expose the PII that it collected and maintained.

118. Francesca's was clearly aware of the risks it was taking and the harm that could result from inadequate data security, and it could have prevented this Data Breach.

119. Data disclosures and data breaches are preventable.[37] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[38] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised[.]"[39]

120. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[40]

---

[32] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.
[33] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.
[34] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/.
[35] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.
[36] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.
[37] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[38] *Id.* at 17.
[39] *Id.* at 28.
[40] *Id.*

121. In a Data Breach like this, many failures laid the groundwork for the Breach. The FTC published guidelines that establish reasonable data security practices for businesses. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[41] The guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommended that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

122. Upon information and belief, Francesca's failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines. Upon information and belief, Francesca's also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

123. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[42]

124. To prevent and detect ransomware attacks, including the ransomware attack that

[41] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[42] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

resulted in the Data Breach, Francesca's could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[43]

125. The threat continues. In August 2022, the Consumer Finance Protection Bureau (CFPB) published a circular on data security. The CFPB noted that "[w]idespread data breaches and cyberattacks have resulted in significant harms to consumers, including monetary loss, identity theft, significant time and money spent dealing with the impacts of the breach, and other forms of financial distress," and the circular concluded that the provision of insufficient security for consumers' data can violate the prohibition on "unfair acts or practices" in the Consumer Finance Protection Act (CFPA).

126. Further, to prevent and detect ransomware attacks, Francesca's could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) ….

[43] *Id.* at 3-4.

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic. . . .[44]

127. In addition, to prevent and detect ransomware attacks, Francesca's could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
    - Apply latest security updates
    - Use threat and vulnerability management
    - Perform regular audits; remove privileged credentials
- **Thoroughly investigate and remediate alerts**
    - Prioritize and treat commodity malware infections as potential full compromises;
- **Include IT Pros in security discussions**

[44] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001.

- Ensure collaboration among [security operations], [security admins], and [information technology admins to configure servers and other endpoints securely;

- **Build credential hygiene**

  - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

- **Apply principle of least-privilege**

  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events

- **Harden infrastructure**

  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[45]

128. Given that Francesca's was storing the PII of at least 50,000 individuals, Francesca's could and should have implemented all of the above measures to prevent and detect ransomware attacks. These are basic, common-sense email security measures that every business, not only retail businesses, should be doing. Francesca's, with its heightened standard of care should be doing even more.

129. Specifically, among other failures, Defendants had far too much confidential unencrypted information held on their network and systems. Such PII should have been segregated into an encrypted system.[46] Indeed, the United States Department of Health and Human Services'

[45] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

[46] *See, e.g.,* Adnan Raja, *How to Safeguard Your Business Data with Encryption*, Aug. 14, 2018, https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption.

Office for Civil Rights urges the use of encryption of data containing sensitive personal information, stating "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[47]

130. Charged with handling sensitive PII, including financial information, Defendants knew, or should have known, the importance of safeguarding their employees' and customers' PII that was entrusted to them, and of the foreseeable consequences if their data security systems were breached. This includes the significant costs that would be imposed on their current and former employees and customers after a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

131. With respect to training, Defendants specifically failed to:

- Implement a variety of anti-ransomware training tools, in combination, such as computer-based training, classroom training, monthly newsletters, posters, login alerts, email alerts, and team-based discussions;
- Perform regular training at defined intervals such as bi-annual training and/or monthly security updates; and
- Craft and tailor different approaches to different employees based on their base knowledge about technology and cybersecurity.

132. The PII was also maintained on Francesca's computer system in a condition vulnerable to cyberattacks, such as through the infiltration of Defendants' systems through ransomware attacks. The mechanism of the cyberattack and the potential for improper disclosure of Plaintiffs' and Class Members' PII was a known risk to Francesca's, and thus Francesca's was on notice that failing to take reasonable steps necessary to secure the PII from those risks left it in a vulnerable position.

[47]"Stolen Laptops Lead to Important HIPAA Settlements," U.S. Dep't of Health and Human Services (Apr. 22, 2014), available at https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

133. In sum, this Data Breach could have readily been prevented by employing industry standard network segmentation and encryption of all confidential information.

134. Plaintiffs and Class Members entrusted their PII to Francesca's as a condition of employment and to receive retail services. Plaintiffs and Class Members understood and expected that Francesca's or anyone in Defendants' position would safeguard their PII against cyberattacks, delete or destroy PII that Francesca's was no longer required to maintain, and timely and accurately notify them if their PII was compromised.

## I. The Monetary Value of Privacy Protections and Private Information

135. The fact that Plaintiffs' and Class Members' PII was stolen means that their PII is likely for sale by cybercriminals and will be further misused in the future. Indeed, there is already evidence that Plaintiffs' PII is on the dark web.

136. At all relevant times, Defendants were well aware that the PII they collect from Plaintiffs and Class Members is highly sensitive and of significant value to those who would use it for wrongful purposes.

137. As discussed above, PII is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud.[48]

138. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood,

[48] Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed November 30, 2022).

the free flow of information.[49]

139. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 Billion per year online advertising industry in the United States.[50]

140. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[51]

141. Recognizing the high value that consumers place on their PII, many companies now offer consumers an opportunity to sell this information.[52] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their PII. This business has created a new market for the sale and purchase of this valuable data.

142. Consumers place a high value not only on their PII, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of

---

49 *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, FED. TRADE COMM'N Tr. at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last accessed November 30, 2022).

50 *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), https://allthingsd.com/20110228/webs-hot-new-commodity-privacy/ [hereinafter *Web's New Hot Commodity*].

51 *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last accessed November 30, 2022).

52 *Web's Hot New Commodity*, *supra*.

identity theft in 2014 was $1,349.[53]

143. As discussed above, the value of Plaintiffs' and Class Members' PII on the black market is substantial.

144. The ramifications of Defendants' failure to keep Plaintiffs' and Class Members' PII secure are long-lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

145. Victims may not realize their identity has been compromised until long after it has happened.[54] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[55]

146. At all relevant times, Defendants were well-aware, or reasonably should have been aware, that the PII they maintain is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud.

147. Had Defendants remedied the deficiencies in their security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendants would have prevented the ransomware attack into their systems and, ultimately, the theft of their employees' and customers' PII.

148. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves. Indeed, "there is

[53] *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*] (last accessed November 30, 2022).

[54] *See, e.g.*, *Survey on Medical Identity Theft*, Ponemon Institute, June 2012, https://www.ponemon.org/local/upload/file/Third_Annual_Survey_on_Medical_Identity_Theft_FINAL.pdf (last accessed November 30, 2022).

[55] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches*, EXPERIAN, (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last accessed November 30, 2022).

significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[56] For example, different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[57] Based upon information and belief, the unauthorized parties utilized the PII they obtained through the Data Breach to obtain additional information from Plaintiffs and Class Members that was misused.

149. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

150. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if payment card information was not involved in the Data Breach, though it was here, the unauthorized parties could use Plaintiffs' and Class Members' PII to access accounts, including, but not limited to email accounts and financial accounts, to engage in the fraudulent activity identified by Plaintiffs.

151. Given these facts, any retail or other type of entity that transacts business with customers and then compromises the privacy of its customers' PII has thus deprived them of the full monetary value of the transaction with the entity.

152. Acknowledging the damage to Plaintiffs and Class Members, Defendants instructed current and former employees and customers like Plaintiffs to "remain vigilant against incidents of

[56] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, FED. TRADE COMM'N 35-38 (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework (last accessed November 30, 2022).
[57] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

identity theft and fraud[.]" Plaintiffs and Class Members now face an impending, substantial risk of identity theft and financial fraud.

153. In short, the PII exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

**J. The Data Breach's Impact on Plaintiffs and Class Members**

154. Francesca's received Plaintiffs' PII in connection with employment and/or by providing certain services to them. In requesting and maintaining Plaintiffs' PII for business purposes, Francesca's expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiffs' PII. Francesca's, however, did not take proper care of Plaintiffs' PII, leading to its exposure to and exfiltration by cybercriminals as a direct result of Francesca's inadequate data security measures.

155. On or around September 25, 2023, Francesca's sent Plaintiffs notice concerning the Data Breach. The letter stated that Francesca's experienced a cybersecurity attack and that the incident may have resulted in unauthorized access to Plaintiffs' PII stored on Francesca's systems. The notice stated that the compromised information that was present on the impacted files included one or more of the following data elements: first and last names, Social Security numbers, and financial account information. The notice further encouraged that Plaintiffs and Class Members "remain vigilant against incidents of identity theft and fraud by regularly reviewing your credit reports/account statements for suspicious activity and to detect errors." Francesca's also offered identity theft protection services through Kroll, but only for a period of one year.

156. Defendants' conduct, which allowed the Data Breach to occur, caused Plaintiffs significant injuries and harm, including but not limited to, the following—Plaintiffs immediately devoted (and must continue to devote) time, energy, and money to: closely monitoring their bills,

records, and credit and financial accounts; changing login and password information on any sensitive account even more frequently than they already do; more carefully screening and scrutinizing phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; searching for suitable identity theft protection and credit monitoring services and paying for such services to protect themselves; and placing fraud alerts and/or credit freezes on their credit file. Plaintiffs have taken or will be forced to take these measures in order to mitigate their potential damages as a result of the Breach.

157. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs must maintain these heightened measures for years, and possibly their entire lives. Consumer victims of data breaches are more likely to become victims of identity fraud.[58]

158. Plaintiffs and Class Members greatly value their privacy, especially while receiving retail services. Plaintiffs and Class Members did not receive the full benefit of their bargain when paying for retail services, and instead received services that were of a diminished value to those described in their agreements with Francesca's for the benefit and protection of Plaintiffs and Class Members and their respective PII. Plaintiffs and Class Members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they actually received.

159. Plaintiffs and Class Members would not have obtained employment or retail services from Francesca's, or paid the amount they did to receive such, had they known that Francesca's would negligently fail to adequately protect their PII. Indeed, Plaintiffs paid, or contracted with, Francesca's for employment and/or retail services with the expectation that Francesca's would keep their PII

[58] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

secure and inaccessible from unauthorized parties. Plaintiffs and Class Members would not have obtained employment and/or retail services from Francesca's had they known that Defendants failed to properly train their employees, lacked safety controls over their computer network, and did not have proper data security practices to safeguard their Private Information from criminal theft and misuse.

160. Plaintiffs and Class Members have lost confidence in Francesca's as a result of the Data Breach.

161. As a direct result of Defendants' intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise commit the identity theft and misuse of Plaintiffs' and Class Members' PII as detailed above, and Plaintiffs and members of the Class are at a heightened and increased substantial risk of suffering identity theft and fraud.

162. Plaintiffs and Class Members are also at a continued risk of harm because their PII remains in Francesca's' systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Francesca's fails to undertake the necessary and appropriate data security measures to protect the PII in its possession.

163. As a result of the Data Breach, and in addition to the time Plaintiffs and Class Members have spent and anticipate spending to mitigate the impact of the Data Breach on their lives, Plaintiffs have also suffered emotional distress from the public release of their PII, which they believed would be protected from unauthorized access and disclosure. The emotional distress they have experienced includes anxiety and stress resulting from the unauthorized bad actors viewing, selling, and misusing their PII for the purposes of identity theft and fraud.

164. Plaintiffs and Class Members have suffered damage to and diminution in the value of their highly sensitive and confidential PII—a form of property that Plaintiffs and Class Members

entrusted to Francesca's and which was compromised as a result of the Data Breach Francesca's failed to prevent. Plaintiffs and Class Members have also suffered a violation of their privacy rights as a result of Francesca's unauthorized disclosure of their PII.

165. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

166. Some of the injuries and risks associated with the loss of PII have already manifested themselves in Plaintiffs' and other Class Members' lives. Each Class Member received a cryptically written notice letter from Defendants stating that their PII was released, and that they should remain vigilant for fraudulent activity, with no other explanation of where this PII could have gone, or who might have access to it.

167. In addition to a remedy for the economic harm, Plaintiff and Class Members maintain an undeniable interest in ensuring that their PII remains secure and is not subject to further misappropriation and theft.

**K. Plaintiffs' Experiences**

*Plaintiff Taylor Doherty's Experience*

168. Plaintiff Doherty is a former employee and customer of Francesca's. As a condition of employment with, and purchasing from, Francesca's, Plaintiff Doherty was required to give her Private Information to Francesca's.

169. Plaintiff Doherty is very careful about sharing her Private Information. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

Plaintiff Doherty stores any documents containing her sensitive PII in a safe and secure location or destroys the documents.

170. Plaintiff Doherty only allowed Defendants to maintain, store, and use her Private Information because she believed that Defendants would use basic, industry standard data security measures, such as those set forth herein, to protect it from unauthorized access.

171. Plaintiff Doherty received the Notice of Data Breach on or around September 25, 2023, stating, in relevant part, that her Social Security number and financial account information were compromised in the Data Breach.

172. Plaintiff Doherty now faces a continued risk of harm that is not only imminent but has already happened in Plaintiff Doherty's case, as she recently began receiving incessant amounts of phishing emails and text messages. She has also had hackers attempt to use her email account to manipulate two-factor authentication and gain access to other accounts where additional sensitive information is stored. Additionally, multiple applications on her phone were accessed without her authorization, resulting in Plaintiff Doherty having to spend time changing passwords to emails, insurance and medical accounts, social media accounts, and others. Plaintiff Doherty was also forced to pay for credit monitoring and identity theft protection services before she became aware of Defendants' offer of abbreviated credit monitoring of unknown quality due to these instances of misuse of her PII that she experienced (and Defendants' 8-month delay in sending Plaintiffs and Class Members notice of the Data Breach).

173. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, in addition to the increased, imminent, and substantial risk of a future data breach and harm, Plaintiff Doherty will need to maintain these heightened measures for years, and possibly her entire life.

174. Plaintiff Doherty greatly values her privacy, especially while seeking employment and receiving retail services. She would not have obtained employment or retail services from Francesca's had she known that Francesca's would negligently fail to adequately protect her PII. Indeed, Plaintiff Doherty paid Francesca's for retail services with the expectation that Francesca's would keep her PII secure and inaccessible from unauthorized parties, as promised by Francesca's.

175. Plaintiff Doherty is also at a continued imminent and substantial risk of harm because her PII remains in Francesca's systems, which have already been shown to be susceptible to compromise and attack and are subject to an increased and imminent future attack.

176. As a result of the Data Breach, and in addition to the time Plaintiff Doherty has spent and anticipates spending to mitigate the impact of the Data Breach on her life, Plaintiff Doherty also suffered emotional distress from the public release of her PII, which she believed would be protected from unauthorized access and disclosure. The emotional distress she experienced, and will continue to experience, includes anxiety and stress resulting from the unauthorized bad actors viewing, selling, and misusing her PII for the purposes of identity theft and fraud.

177. Additionally, Plaintiff Doherty has suffered damage to and diminution in the value of her highly sensitive and confidential PII—a form of property that Plaintiff Doherty provided and entrusted to Francesca's, and which was compromised as a result of the Data Breach Francesca's failed to prevent. Plaintiff Doherty has also suffered a violation of her privacy rights as a result of Francesca's' unauthorized disclosure of her PII.

178. The free credit monitoring and identity restoration services offered by Francesca's after the Data Breach came far too late and were (and continue to be) woefully insufficient.

179. The time spent dealing with the repercussions of the Data Breach is time Plaintiff Doherty otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff lost was spent at Francesca's direction. Indeed, in the notice letter Plaintiff received,

Francesca's directed Plaintiff to spend time by reviewing her accounts and credit reports for unauthorized activity.

*Plaintiff Alessandra Jimenez's Experience*

180. Plaintiff Jimenez is a former employee and customer of Francesca's. As a condition of employment with, and purchasing from, Francesca's, Plaintiff Jimenez was required to give her Private Information to Francesca's.

181. Plaintiff Jimenez is very careful about sharing her Private Information. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Jimenez stores any documents containing her sensitive PII in a safe and secure location or destroys the documents.

182. Plaintiff Jimenez only allowed Defendants to maintain, store, and use her Private Information because she believed that Defendants would use basic, industry standard data security measures, such as those set forth herein, to protect it from unauthorized access.

183. Plaintiff Jimenez received the Notice of Data Breach on or around September 25, 2023, stating, in relevant part, that her Social Security number and financial account information were disclosed in the Data Breach.

184. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, in addition to the increased, imminent, and substantial risk of a future data breach and harm, Plaintiff Jimenez will need to maintain these heightened measures for years, and possibly her entire life.

185. Plaintiff Jimenez greatly values her privacy, especially while receiving retail services. She would not have obtained retail services from Francesca's, or paid the amount she did to receive such, had she known that Francesca's would negligently fail to adequately protect her PII. Indeed,

Plaintiff Jimenez paid Francesca's for retail services with the expectation that Francesca's would keep her PII secure and inaccessible from unauthorized parties, as promised by Francesca's.

186. Plaintiff Jimenez is also at a continued imminent and substantial risk of harm because her PII remains in Francesca's' systems, which have already been shown to be susceptible to compromise and attack and are subject to an increased and imminent future attack.

187. As a result of the Data Breach, and in addition to the time Plaintiff Jimenez has spent and anticipates spending to mitigate the impact of the Data Breach on her life, Plaintiff Jimenez also suffered emotional distress from the public release of her PII, which she believed would be protected from unauthorized access and disclosure. The emotional distress she experienced, and will continue to experience, includes anxiety and stress resulting from the unauthorized bad actors viewing, selling, and misusing her PII for the purposes of identity theft and fraud.

188. Additionally, Plaintiff Jimenez has suffered damage to and diminution in the value of her highly sensitive and confidential PII—a form of property that Plaintiff Jimenez provided and entrusted to Francesca's, and which was compromised as a result of the Data Breach Francesca's failed to prevent. Plaintiff Jimenez has also suffered a violation of her privacy rights as a result of Francesca's' unauthorized disclosure of her PII.

189. The free credit monitoring and identity restoration services offered by Francesca's after the Data Breach were and continue to be ineffective because these services would have shared Plaintiff Jimenez's information with third parties and could not guarantee complete privacy of her sensitive information.

190. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Jimenez otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff lost was spent at Francesca's direction. Indeed, in the notice letter Plaintiff

received, Francesca's directed Plaintiff to spend time by reviewing her accounts and credit reports for unauthorized activity.

*Plaintiff Kayla Stewart's Experience*

191. Plaintiff Stewart is a former employee and customer of Francesca's. As a condition of employment with, and purchasing from, Francesca's, Plaintiff Stewart was required to give her Private Information to Francesca's.

192. Plaintiff Stewart is very careful about sharing her Private Information. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Stewart stores any documents containing her sensitive PII in a safe and secure location or destroys the documents.

193. Plaintiff Stewart only allowed Defendants to maintain, store, and use her Private Information because she believed that Defendants would use basic, industry standard data security measures, such as those set forth herein, to protect it from unauthorized access.

194. Plaintiff Stewart received the Notice of Data Breach on or around September 25, 2023, stating, in relevant part, that her Social Security number and financial account information were disclosed in the Data Breach.

195. Plaintiff Stewart now faces a continued risk of harm that is not only imminent but has already happened in Plaintiff Stewart's case, as she recently experienced identity fraud following the Data Breach when a credit card was opened in her name, a concrete injury.

196. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, in addition to the increased, imminent, and substantial risk of a future data breach and harm, Plaintiff Stewart will need to maintain these heightened measures for years, and possibly her entire life.

197. Plaintiff Stewart greatly values her privacy, especially while receiving retail services. She would not have obtained retail services from Francesca's, or paid the amount she did to receive such, had she known that Francesca's would negligently fail to adequately protect her PII. Indeed, Plaintiff Stewart paid Francesca's for retail services with the expectation that Francesca's would keep her PII secure and inaccessible from unauthorized parties, as promised by Francesca's.

198. Plaintiff Stewart is also at a continued imminent and substantial risk of harm because her PII remains in Francesca's systems, which have already been shown to be susceptible to compromise and attack and are subject to an increased and imminent future attack.

199. As a result of the Data Breach, and in addition to the time Plaintiff Stewart has spent and anticipates spending to mitigate the impact of the Data Breach on her life, Plaintiff Stewart also suffered emotional distress from the public release of her PII, which she believed would be protected from unauthorized access and disclosure. The emotional distress she experienced, and will continue to experience, includes anxiety and stress resulting from the unauthorized bad actors viewing, selling, and misusing her PII for the purposes of identity theft and fraud.

200. Additionally, Plaintiff Stewart has suffered damage to and diminution in the value of her highly sensitive and confidential PII—a form of property that Plaintiff Stewart provided and entrusted to Francesca's, and which was compromised as a result of the Data Breach Francesca's failed to prevent. Plaintiff Stewart has also suffered a violation of her privacy rights as a result of Francesca's' unauthorized disclosure of her PII.

201. The free credit monitoring and identity restoration services offered by Francesca's after the Data Breach were and continue to be ineffective because these services would have shared Plaintiff Stewart's information with third parties and could not guarantee complete privacy of her sensitive information.

202. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Stewart otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff lost was spent at Francesca's' direction. Indeed, in the notice letter Plaintiff received, Francesca's directed Plaintiff to spend time by reviewing her accounts and credit reports for unauthorized activity.

*Plaintiff Ellie Bley's Experience*

203. Plaintiff Ellie Bley is a former employee and customer of Francesca's. Plaintiff Bley was employed by Francesca's from 2017 to 2018. As a condition of employment with, and purchasing from, Francesca's, Plaintiff Bley was required to give her Private Information to Francesca's.

204. Plaintiff Bley is very careful about sharing her Private Information. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Bley stores any documents containing her sensitive PII in a safe and secure location or destroys the documents.

205. Plaintiff Bley only allowed Defendants to maintain, store, and use her Private Information because she believed that Defendants would use basic, industry standard data security measures, such as those set forth herein, to protect it from unauthorized access.

206. Plaintiff Bley received the Notice of Data Breach on or around September 25, 2023, stating, in relevant part, that her Social Security number and financial account information were disclosed in the Data Breach.

207. After the breach, Plaintiff Bley experienced a dramatic increase in the number of spam phone calls and emails.

208. As a result of the Data Breach and the resulting suspicious activity, Plaintiff Bley made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of

actual or attempted identity theft or fraud. She has also spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including, but not limited to, work and recreation.

209. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, in addition to the increased, imminent, and substantial risk of a future data breach and harm, Plaintiff Bley will need to maintain these heightened measures for years, and possibly her entire life.

210. Plaintiff Bley greatly values her privacy, especially while receiving retail services. She would not have obtained retail services from Francesca's, or paid the amount she did to receive such, had she known that Francesca's would negligently fail to adequately protect her PII. Indeed, Plaintiff Bley paid Francesca's for retail services with the expectation that Francesca's would keep her PII secure and inaccessible from unauthorized parties, as promised by Francesca's.

211. Plaintiff Bley is also at a continued imminent and substantial risk of harm because her PII remains in Francesca's' systems, which have already been shown to be susceptible to compromise and attack and are subject to an increased and imminent future attack.

212. As a result of the Data Breach, and in addition to the time Plaintiff Bley has spent and anticipates spending to mitigate the impact of the Data Breach on her life, Plaintiff Bley also suffered emotional distress from the public release of her PII, which she believed would be protected from unauthorized access and disclosure. The emotional distress she experienced, and will continue to experience, includes anxiety and stress resulting from the unauthorized bad actors viewing, selling, and misusing her PII for the purposes of identity theft and fraud.

213. Additionally, Plaintiff Bley suffered damage to and diminution in the value of her highly sensitive and confidential PII—a form of property that Plaintiff Bley provided and entrusted to Francesca's, and which was compromised as a result of the Data Breach Francesca's failed to

prevent. Plaintiff Bley also suffered a violation of her privacy rights as a result of Francesca's' unauthorized disclosure of her PII.

214. The free credit monitoring and identity restoration services offered by Francesca's after the Data Breach were and continue to be ineffective because these services would have shared Plaintiff Bley's information with third parties and could not guarantee complete privacy of her sensitive information.

215. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Bley otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff lost was spent at Francesca's' direction. Indeed, in the notice letter Plaintiff received, Francesca's directed Plaintiff to spend time by reviewing her accounts and credit reports for unauthorized activity.

*Plaintiff Wendy Nolasco's Experience*

216. Plaintiff Nolasco was employed by Francesca's in San Diego, California from November 2022 to January 2023. During her employment with the Defendant, she made purchases of approximately $15 with her debit card.

217. As a condition of her employment, Plaintiff Nolasco was required to provide her Private Information to Francesca's.

218. Plaintiff Nolasco is very careful about sharing her Private Information. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Nolasco stores any documents containing her sensitive PII in a safe and secure location or destroys the documents.

219. Plaintiff Nolasco only allowed Defendants to maintain, store, and use her Private Information because she believed that Defendants would use basic, industry standard data security measures, such as those set forth herein, to protect it from unauthorized access.

220. Plaintiff Nolasco suffered, and continues to suffer from, actual and imminent identity theft and misuse of her PII as a direct and/or proximate result of Francesca's actions and inactions.

221. Francesca's conduct, which allowed the Data Breach to occur, caused Plaintiff Nolasco significant injuries and harm, including but not limited to, the following—Plaintiff Nolasco immediately devoted (and must continue to devote) time, energy, and money to: closely monitor her bills, records, and credit and financial accounts; change login and password information on any sensitive account even more frequently than she already does; more carefully screen and scrutinize phone calls, emails, and other communications to ensure that she is not being targeted in a social engineering or spear phishing attack; search for suitable identity theft protection and credit monitoring services and paying for such services to protect herself; and place fraud alerts and/or credit freezes on her credit file. Ms. Nolasco has taken or will be forced to take these measures in order to mitigate her potential damages that are fairly traceable to the Data Breach.

222. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, in addition to the increased, imminent, and substantial risk of a future data breach and harm, Plaintiff Nolasco will need to maintain these heightened measures for years, and possibly her entire life.

223. Plaintiff Nolasco greatly values her privacy, especially while receiving retail services. She would not have obtained retail services from Francesca's, or paid the amount she did to receive such, had she known that Francesca's would negligently fail to adequately protect her PII. Indeed, Plaintiff Nolasco paid Francesca's for retail services with the expectation that Francesca's would keep her PII secure and inaccessible from unauthorized parties, as promised by Francesca's.

224. Plaintiff Nolasco is also at a continued imminent and substantial risk of harm because her PII remains in Francesca's' systems, which have already been shown to be susceptible to compromise and attack and are subject to an increased and imminent future attack.

225. As a result of the Data Breach, and in addition to the time Plaintiff Nolasco has spent and anticipates spending to mitigate the impact of the Data Breach on her life, Plaintiff Nolasco also suffered emotional distress from the public release of her PII, which she believed would be protected from unauthorized access and disclosure. The emotional distress she experienced, and will continue to experience, includes anxiety and stress resulting from the unauthorized bad actors viewing, selling, and misusing her PII for the purposes of identity theft and fraud.

226. Additionally, Plaintiff Nolasco has suffered damage to and diminution in the value of her highly sensitive and confidential PII—a form of property that Plaintiff Nolasco provided and entrusted to Francesca's, and which was compromised as a result of the Data Breach Francesca's failed to prevent. Plaintiff Nolasco has also suffered a violation of her privacy rights as a result of Francesca's' unauthorized disclosure of her PII.

227. The free credit monitoring and identity restoration services offered by Francesca's after the Data Breach were and continue to be ineffective because these services would have shared Plaintiff Nolasco's information with third parties and could not guarantee complete privacy of her sensitive information.

228. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Nolasco otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff lost was spent at Francesca's' direction. Indeed, in the notice letter Plaintiff received, Francesca's directed Plaintiff to spend time by reviewing her accounts and credit reports for unauthorized activity.

229. The Private Information maintained by and stolen from Defendants' systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which has been and will continue to be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

230. Further, as a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have been forced to spend time dealing with the effects of the Data Breach. Specifically, Plaintiff and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

231. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit free fees, and similar costs directly or indirectly related to the Data Breach.

232. Plaintiffs and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach.[59] Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion. In fact, consumers who agree to provide their web browsing history to the Nielsen corporation can in turn receive up to $50 a year.[60]

233. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the

[59] *See* https://thequantumrecord.com/blog/data-brokers-profit-from-ourdata/#:~:text=The%20business%20of%20data%20brokering,annual%20revenue%20of%20%24200%20billion (last visited on October 9, 2023).
[60] Frequently Asked Questions, Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited on October 9, 2023).

Private Information has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

234. Finally, Plaintiffs and Class members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

235. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Francesca's, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

236. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial risk of harm, in the forms set forth above.

## CLASS ACTION ALLEGATIONS

237. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(3), and/or 23(c)(4).

238. Specifically, Plaintiffs propose the following Nationwide Class, as well as the below State Subclasses (collectively, the "Class"):

**Nationwide Class**

> All persons residing in the United States whose PII was compromised as a result of the Data Breach discovered on or about January 2023, including all who were sent a notice of the Data Breach, by the Defendant Francesca's Acquisition, LLC.

**California Subclass**

All persons residing in California whose PII was compromised as a result of the Data Breach discovered on or about January 2023, including all California residents who were sent notice of the Data Breach by the Defendant Francesca's Acquisition, LLC.

**Massachusetts Subclass**

All persons residing in Massachusetts whose PII was compromised as a result of the Data Breach discovered on or about January 2023, including all Massachusetts residents who were sent notice of the Data Breach by the Defendant Francesca's Acquisition, LLC.

**Illinois Subclass**

All persons residing in Illinois whose PII was compromised as a result of the Data Breach discovered on or about January 2023, including all Illinois residents who were sent notice of the Data Breach by the Defendant Francesca's Acquisition, LLC.

**Maryland Subclass**

All persons residing in Maryland whose PII was compromised as a result of the Data Breach discovered on or about January 2023, including all Maryland residents who were sent notice of the Data Breach by the Defendant Francesca's Acquisition, LLC.

**Pennsylvania Subclass**
All persons residing in Pennsylvania whose PII was compromised as a result of the Data Breach discovered on or about January 2023, including all Pennsylvania residents who were sent notice of the Data Breach by the Defendant Francesca's Acquisition, LLC.

239. Excluded from the Class are the (i) owners, officers, directors, employees, agents and/or representatives of Defendants and their parent entities, subsidiaries, affiliates, successors, and/or assigns, and (ii) the Court, Court personnel, and members of their immediate families.

240. Plaintiffs reserve the right to modify, change, amend, or expand the definitions of the Nationwide Class, as well as the Subclasses, based upon discovery and further investigation.

241. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiff can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

242. **Numerosity – Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class Members would be impracticable. On information and belief, the Nationwide Class number is at least 58,387 individuals. The identities of Class members are ascertainable through Defendants' records, Class Members' records, publication notice, self-identification, and other means.

243. **Commonality and Predominance – Federal Rule of Civil Procedure 23(a)(2).** Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

a. Whether Francesca's willfully, recklessly, negligently and/or wantonly failed to maintain and/or execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and Class Members' PII;

b. Whether Francesca's was negligent or wanton in the manner in which it stored Plaintiffs' and Class Members' PII;

c. Whether Francesca's owed a duty to Plaintiffs and Class Members to exercise reasonable care in protecting and securing their PII;

d. Whether Francesca's breached its duty to exercise reasonable care in protecting and securing Plaintiffs' and Class Members' PII;

e. Whether Francesca's was negligent in failing to secure Plaintiffs' and Class Members' PII;

f. Whether Francesca's failure to comply with Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45) constitutes negligence *per se*;

g. Whether Francesca's breached its contracts by failing to maintain the privacy and security of Plaintiffs' and Class Members' PII;

h. Whether by publicly disclosing Plaintiffs' and Class Members' PII without authorization, Francesca's invaded Plaintiffs' and Class Members' privacy;

i. Whether by publicly disclosing Plaintiffs' and Class Members' PII without authorization, Francesca's breached the duty of confidence it owed to Plaintiffs and Class Members;

j. Whether by publicly disclosing Plaintiffs' and Class Members' PII without authorization, Francesca's breached the fiduciary duties it owed to Plaintiffs and Class Members;

k. Whether Francesca's was unjustly enriched when it took money from Plaintiffs and Class Members and failed to provide reasonable data security measures to protect Plaintiffs' and Class Members' PII;

l. Whether Plaintiffs and Class Members sustained damages as a result of Francesca's failure to secure and protect their PII; and,

m. Whether injunctive relief is necessary to ensure Francesca's implements reasonable security measures to protect the PII of Plaintiffs and the Class Members against any future data breaches by Francesca's.

244. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

245. **Typicality – Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the claims of the other members of the Class because, among other things, all Class Members were similarly injured through Defendants' uniform misconduct described above and were thus all subject

to the Data Breach alleged herein. Further, there are no defenses available to Defendants that are unique to Plaintiffs.

246. **Adequacy of Representation – Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and they will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiffs and their counsel.

247. **Injunctive Relief – Federal Rule of Civil Procedure 23(b)(2).** Defendants have acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. R. Civ. P. 23 (b)(2).

248. **Superiority – Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for members of the Class to individually seek redress for Defendants' wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

## CAUSES OF ACTION
## COUNT I
## NEGLIGENCE
## (BY PLAINTIFFS ON BEHALF OF THE CLASS, OR, IN THE ALTERNATIVE, THE STATE SUBCLASSES)

249. Plaintiffs restate and reallege allegations stated in the preceding paragraph as if fully set forth herein.

250. Francesca's knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Private Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

251. Defendants owed a duty of care not to subject Plaintiffs' and the Class's PII to an unreasonable risk of exposure and theft because Plaintiffs and the Class were foreseeable and probable victims of any inadequate security practices.

252. Defendants owed numerous duties to Plaintiffs and the Class, including the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PII in its possession;

b. To protect PII using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

253. Defendants also breached their duty to Plaintiffs and Class Members to adequately protect and safeguard PII by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII. Furthering its dilatory practices, Defendants failed to provide adequate supervision and oversight of the PII with which it was and is entrusted, despite the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiffs and Class Members' PII and misuse the PII and intentionally disclose it to others without consent.

254. Defendants knew, or should have known, of the risks inherent in collecting and storing PII and the importance of adequate security. Defendants knew or should have known about numerous well-publicized data breaches within the retail industry.

255. Defendants knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiffs and Class Members' PII.

256. Defendants breached their duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

257. Because Defendants knew that a breach of their systems would damage thousands of their customers' PII, including Plaintiffs' and Class Members', Defendants had a duty to adequately protect their data systems and the PII contained thereon.

258. Defendants' duty of care to use reasonable security measures arose because of the special relationship that existed between Defendants and its employees, which is recognized by statute, regulations, and the common law. Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class Members from a data breach.

259. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

260. Defendants' own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their PII. Defendants' misconduct included failing to: (1) secure Plaintiffs' and Class Members' PII; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to

prevent this type of data breach.

261. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' PII and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of Defendants' networks and systems;

c. Allowing unauthorized access to Class Members' PII; and

d. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

262. Through Defendants' acts and omissions described in this Complaint, including their failure to provide adequate security and their failure to protect Plaintiffs' and Class Members' PII from being foreseeably captured, accessed, disseminated, stolen and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiffs' and Class Members' PII during the time it was within Defendants' possession or control.

263. Defendants' conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to failing to adequately protect the PII and failing to provide Plaintiffs and Class Members with timely notice that their sensitive Private Information had been compromised.

264. Neither Plaintiffs nor the other Class Members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

265. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class Members suffered damages as alleged above.

266. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, *inter alia*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free credit monitoring to all Class Members.

**COUNT II**
**NEGLIGENCE *PER SE***
**(BY PLAINTIFFS ON BEHALF OF THE CLASS, OR, IN THE ALTERNATIVE, THE STATE SUBCLASSES)**

267. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

268. Section 5 of the FTCA imposes a duty on Defendants to provide fair and adequate data security to secure, protect, and/or otherwise safeguard the Private Information of Plaintiffs and Class Members.

269. Defendants violated the FTCA and state rules and regulations by failing to provide fair, reasonable, or adequate computer systems and data security practices to secure, protect, and/or otherwise safeguard Plaintiffs' and Class Members' Private Information.

270. Defendants' failure to comply with the FTCA and applicable state rules and regulations constitutes negligence *per se*.

271. Plaintiffs and Class Members are within the class of persons that the FTCA and state rules and regulations are intended to protect.

272. It was reasonably foreseeable that the failure to protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws and industry standards would result in that Private Information being accessed and stolen by unauthorized actors.

273. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to theft of their personal information, damages from the lost time and effort to mitigate the impact of the Data Breach, and permanently increased

risk of identity theft.

274. Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial and injunctive relief requiring Defendants to, *inter alia*, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

## COUNT III
## INVASION OF PRIVACY
## (BY PLAINTIFFS ON BEHALF OF THE CLASS, OR, IN THE ALTERNATIVE, THE STATE SUBCLASSES)

275. Plaintiffs restate and reallege allegations stated from the preceding paragraphs as if fully set forth herein.

276. Plaintiffs and Class Members maintain a privacy interest in their Private Information, which is highly sensitive, confidential information that is also protected from disclosure by applicable laws and industry standards, as set forth above.

277. Plaintiffs' and Class Members' PII was contained, stored, and managed electronically in Defendants' records, computers, and databases and was intended to be secured from unauthorized access to third parties because highly sensitive, confidential matters regarding Plaintiffs' and Class Members' identities were only shared with Defendants for the limited purpose of obtaining employment or retail services.

278. Additionally, Plaintiffs' and Class Members' Private Information is highly attractive to criminals who can nefariously use such Private Information for fraud, identity theft, and other crimes without the victims' knowledge and consent.

279. Defendants' disclosure of Plaintiffs' and Class Members' Private Information to unauthorized third parties by allowing such parties to gain access to their network resulted from Defendants' failure to adequately secure and safeguard Plaintiffs' and Class Members' Private Information. Such failure was the direct and proximate cause of unauthorized intrusions into

Plaintiffs' and Class Members' places of solitude and seclusion that are highly offensive to reasonable persons.

280. Such exploitation of Plaintiffs' and Class Members' Private Information was done for Defendants' business purposes.

281. Defendant's unauthorized disclosure of Plaintiffs' and Class Members' Private Information to criminal third parties permitted the electronic intrusion into private quarters where Plaintiffs' and Class Members' Private Information was stored.

282. Plaintiffs and Class Members have been damaged by Defendants' conduct, including by incurring the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

## COUNT IV
## VIOLATION OF THE CALIFORNIA CONSTITUTION'S RIGHT TO PRIVACY
**Cal. Const., art. I, § 1**
**(BY PLAINTIFF NOLASCO ON BEHALF OF THE CALIFORNIA SUBCLASS)**

283. Plaintiffs restate and reallege allegations stated from the preceding paragraphs as if fully set forth herein.

284. For purposes of this section only, the term "Plaintiff" refers to Plaintiff Nolasco.

285. The California Constitution provides:

> "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possession, and protecting property, and pursuing and obtaining safety, happiness, and privacy." (Cal. Const., art. I. § 1)

286. Plaintiff and the California Subclass have a legally recognized and protected privacy interest in the Private Information provided to and obtained by Defendants, including but not limited to, an interest in precluding the dissemination or misuse of this sensitive and confidential information and the misuse of this information for malicious purposes.

287. Plaintiff and the California Subclass reasonably expected Defendants would prevent the unauthorized viewing, use, manipulation, exfiltration, theft, and disclosure of their Private Information and the substantial, imminent risk of the unauthorized use thereof.

288. Defendants' conduct described herein resulted in a serious invasion of privacy of Plaintiff and the Subclass, as the release of Private Information could highly offend a reasonable individual.

289. As a direct consequence of the actions as identified above, Plaintiff and California Subclass Members suffered harms and losses, including but not limited to, the loss of control over use of their identity, harm to their constitutional right to privacy, lost time dedicated to the investigation and attempt to cure harm to their privacy, the need for future expenses and time dedicated to the recovery and protection of imminent future loss, and privacy injuries associated with having their sensitive Private Information disclosed.

## COUNT V
## VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT
### Cal. Civ. Code § 1798.100, *et seq.*
### (BY PLAINTIFF NOLASCO ON BEHALF OF THE CALIFORNIA SUBCLASS)

290. Plaintiffs restate and reallege allegations stated from the preceding paragraphs as if fully set forth herein.

291. For purposes of this section only, the term "Plaintiff" refers to Plaintiff Nolasco.

292. Francesca's is a corporation organized or operated for the profit or financial benefit of its owners. Defendants collect consumers' Private Information as defined in Cal. Civ. Code § 1798.140.

293. Defendants violated § 1798.150 of the CCPA by failing to prevent Plaintiff's and California Subclass Members' unencrypted Private Information from unauthorized access and

exfiltration, theft, or disclosure as a result of Defendants' violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

294. Defendants have a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff's and California Subclass Members' Private Information. As detailed herein, Defendants failed to do so.

295. As a direct and proximate result of Defendants' acts, Plaintiff's and California Subclass Members' Private Information was subject to unauthorized access and exfiltration, theft, or disclosure.

296. Defendants were put on notice of their violations of the CCPA as admitted by Defendants when Francesca's Acquisition LLC belatedly notified the State of California of the data breach. Plaintiffs also filed Complaints that preceded this consolidated Complaint that sought class-wide relief. Thirty days have passed since Defendants were put on notice and they have failed to provide the necessary class-wide relief. Plaintiff Nolasco has also sent a letter to Defendants further specifying their violations of the CCPA that has not resulted in class-wide relief.

297. Plaintiff and California Subclass Members seek injunctive or other equitable relief to ensure Defendants hereinafter properly safeguard customers' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendants continue to hold customers' Private Information, including Plaintiff's and California Subclass Members' Private Information. Plaintiff and California Subclass Members have an interest in ensuring that their Private Information is reasonably protected, and Defendants have demonstrated a pattern of failing to properly safeguard this information, as evidenced by its multiple failures to notify Plaintiff of its data breach and to take appropriate remedial steps post breach.

298. Plaintiff and the California Subclass seek statutory or actual damages, whichever is greater, as well as all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

**COUNT VI**
**VIOLATION OF THE CALIFORNIA CONSUMER LEGAL REMEDIES ACT**
**Cal. Civ. Code § 1750, *et seq.***
**(BY PLAINTIFF NOLASCO ON BEHALF OF THE CALIFORNIA SUBCLASS)**

299. Plaintiffs restate and reallege allegations stated from the preceding paragraphs as if fully set forth herein.

300. For purposes of this section only, the term "Plaintiff" refers to Plaintiff Nolasco.

301. Defendants are "person[s]," as defined by Cal. Civ. Code § 1761 and § 1770 and have provided "services" as defined by Cal. Civ. Code § 1761(b) and § 1770 and have engaged in a "transaction" as defined by Cal. Civ. Code § 1761 and § 1770.

302. As alleged herein this Complaint, Defendants engaged in unfair or deceptive acts or practices in the conduct of consumer transactions in the conduct of trade or commerce, in violation of Cal. Civ. Code § 1770, including, but not limited to:

- Representing that their services were of a particular standard or quality that they knew or should have known were of another;
- Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and California Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;
- Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;
- Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and California Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;
- Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff's and California Subclass Members' Private Information, and;

- Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach.

303. Defendants' representations and omissions were material because they were likely to deceive reasonable employees about the adequacy of Defendants' data security and ability to protect the confidentiality of its customers' Private Information.

304. Defendants acted intentionally, knowingly, and maliciously to violate California's Consumer Legal Remedies Act, and recklessly disregarded Plaintiff's and California Subclass Members' rights.

305. Defendants' conduct is injurious to the public interest because it violates Cal. Civ. Code § 1770, violates a statute that contains a specific legislation declaration of public interest impact, and/or injured persons and had and has the capacity to injure persons. Further, their conduct affected the public interest, including, upon information and belief, the thousands of Californians affected by the Data Breach.

306. As a direct and proximate result of Defendants' unfair or deceptive acts or practices, Plaintiff and California Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from time and expenses related to monitoring their financial accounts for fraudulent activity; and loss of value of their Private Information.

307. Plaintiff Nolasco has also sent a letter to Defendants informing them of the violations of the CLRA alleged herein.

308. Plaintiff and California Subclass Members accordingly seek all monetary and non-monetary relief allowed by law, including actual damages, injunctive relief, civil penalties, and attorneys' fees and costs.

**COUNT VII**
**VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW ("UCL")**
**Cal. Bus. Prof. Code § 17200, *et seq.***
**(BY PLAINTIFF NOLASCO ON BEHALF OF THE CALIFORNIA SUBCLASS)**

309. Plaintiffs restate and reallege allegations stated from the preceding paragraphs as if fully set forth herein.

310. For purposes of this section only, the term "Plaintiff" refers to Plaintiff Nolasco.

311. Defendants violated California's Unfair Competition Law ("UCL") Cal. Bus. Prof. Code § 17200, *et seq*., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in the UCL, including, but not limited to, the following:

a. By representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Class Members' Personal and financial information from unauthorized disclosure, release, data breach, and theft; representing and advertising that they would and did comply with the requirement of relevant federal and state laws relating to privacy and security of Plaintiff's and Class Members' Private Information; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Private Information;

b. By soliciting and collecting Private Information from Plaintiff and Class Members without adequately protecting or storing Private Information; and

c. By violating the California Customer Records Act, as set forth in further detail below.

312. Defendants' practices were also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities that solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the FTC Act, 15 U.S.C. § 45.

313. As a direct and proximate result of Defendants' unfair and unlawful practices and acts, Plaintiff and the Class were injured and lost money or property, including but not limited to,

overpayments Defendants received to maintain adequate security measures and did not, the loss of their legally protected interest in the confidentiality and privacy of their Private information, and additional losses described above.

314. Defendants knew or should have known that their administrative and data security measures were inadequate to safeguard Plaintiff's and Class Members' Private Information and that the risk of a data breach or unauthorized access was highly likely. Defendants had resources to secure and/or prepare for protecting customers' Private Information in a data breach. Defendants' actions in engaging in the above-named unfair, unlawful and deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of the Class.

315. Plaintiff seeks relief under the UCL, including restitution to the Class of money or property that the Defendants may have acquired by means of their deceptive, unlawful, and unfair business practices, declaratory relief, attorney fees, costs and expenses (pursuant to Cal. Code Civ. P. § 1021.5), and injunctive or other equitable relief.

## COUNT VIII
## VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT ("CRA")
**Cal. Bus. Prof. Code § 1798.80, *et seq.***
**(BY PLAINTIFF NOLASCO ON BEHALF OF THE CALIFORNIA SUBCLASS)**

316. Plaintiffs restate and reallege allegations stated from the preceding paragraphs as if fully set forth herein.

317. For purposes of this section only, the term "Plaintiff" refers to Plaintiff Nolasco.

318. At all relevant times, Defendants were a "business" under the terms of the CRA, operating in the State of California and owning or licensing computerized data that included the Private Information of Plaintiffs and the Class.

319. At all relevant times, Plaintiff and the Class were "customers" under the terms of the CRA as natural persons who provided personal information to Defendants for the purpose of purchasing or leasing a product or obtaining a service from Defendants.

320. Section 1798.82 requires disclosure "shall be made in the most expedient time possible and without unreasonable delay…." By the acts described above, Defendants violated the CRA by allowing unauthorized access to customers' personal and financial information and then failing to inform them for months when the unauthorized use occurred, thereby failing in their duty to inform their customers of unauthorized access expeditiously and without unreasonable delay.

321. The Data Breach described herein is a "breach of the security system" under Section 1798.82.

322. As a direct consequence of the actions as identified above, Plaintiff and the Class incurred additional losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, harm to their constitutional right to privacy, lost time dedicated to the investigation of and attempt to recover the loss of funds and/or cure harm to their privacy, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal and financial information disclosed, that they would have not otherwise lost had Defendants immediately informed them of the unauthorized use.

323. Plaintiff accordingly requests the Court enter an injunction requiring Defendants to implement and maintain reasonable security procedures.

324. Plaintiff further requests the Court require Defendants to identify all of their impacted clients, to what degree their information was stolen, and to notify all members of the Class who have not yet been informed of the Data Breach by written email within 24 hours of discovery of a breach, possible breach, and by mail within 72 hours.

325. As a result of Defendants' violations, Plaintiff and the Class are entitled to all actual and compensatory damages according to proof, to non-economic injunctive relief allowable under the CRA, and to such other and further relief as this Court may deem just and proper.

## COUNT IX
## BREACH OF IMPLIED CONTRACT
**(BY PLAINTIFFS ON BEHALF OF THE CLASS, OR, IN THE ALTERNATIVE, THE STATE SUBCLASSES)**

326. Plaintiffs restate and reallege allegations stated from the preceding paragraphs as if fully set forth herein.

327. Francesca's provided employment, as well as goods and services, to Plaintiffs and Class Members, in exchange for payment and, in the case of its current and former employees, also required Plaintiffs and Class Members to provide Francesca's with their PII in order to receive employment.

328. Francesca's, as an employer and retailer, held the Private Information on behalf of Plaintiffs and Class Members. Holding Plaintiffs' and Class Members' Private Information was part of Defendants' regular business practices, as agreed to by the parties. When Plaintiffs and Class Members joined Defendants' employment and/or purchased products from Defendants, they agreed to have their Private Information stored in Defendants' network.

329. Plaintiffs and Class Members entered implied contracts with Defendants in which Defendants agreed to safeguard and protect such Private Information and to timely detect any breaches of their Private Information. Plaintiffs and Class Members were required to share Private Information to obtain employment and make payments to purchase products from Defendants. In entering such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

330. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Defendants.

331. Defendants' implied promises to Plaintiffs and Class Members include, but are not limited, to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

332. Defendants breached these implied promises they made with Plaintiffs and Class Members by failing to safeguard and protect their Private Information and by failing to notify Plaintiffs and Class Members thereof within a reasonable time.

333. Plaintiffs and Class Members would not have entrusted their Private Information to Francesca's in the absence of such an implied contract.

334. Had Francesca's disclosed to Plaintiffs and the Class that it did not have adequate computer systems and security practices in place to secure such sensitive data, Plaintiffs and Class Members would not have provided their Private Information to Francesca's.

335. Francesca's recognized that Plaintiffs' and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiffs and Class Members.

336. Francesca's violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information.

337. Plaintiffs and Class Members have been damaged by Defendants' conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

338. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, *inter alia*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free lifetime credit monitoring to all Class Members.

## COUNT X
## UNJUST ENRICHMENT
**(BY PLAINTIFFS ON BEHALF OF THE CLASS, OR, IN THE ALTERNATIVE, THE STATE SUBCLASSES)**

339. Plaintiffs restate and reallege allegations stated from the preceding paragraphs as if fully set forth herein.

340. This Count is pleaded in the alternative to Count IX above.

341. Plaintiffs and Class Members conferred a benefit on Defendants. Specifically, they provided Defendants with their Private Information, which Private Information has inherent value. They also provided money to Defendants when making purchases from Defendants. In exchange, Plaintiffs and Class Members should have been entitled to have Defendants protect their Private Information with adequate data security.

342. Defendants knew that Plaintiffs and Class Members conferred these benefits upon them and accepted and retained such benefits by accepting and retaining the Private Information entrusted to them, while also accepting the payments made to them. Defendants profited from Plaintiffs' retained data and used Plaintiffs' and Class Members' Private Information for business purposes.

343. Defendants failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their Private Information provided.

344. Defendants acquired the Private Information through inequitable record retention as they failed to disclose the inadequate security practices previously alleged.

345. If Plaintiffs and Class Members had known that Defendants would not use adequate data security practices, procedures, and protocols to secure their Private Information, they would have made alternative employment and purchasing choices that excluded Defendants.

346. Plaintiffs and Class Members have no adequate remedy at law.

347. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon them.

348. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) the imminent and substantial risk of actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Francesca's fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private

Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

349. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Francesca's and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Francesca's from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

350. Plaintiffs and Class Members may not have an adequate remedy at law against Francesca's, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above, seek the following relief:

A. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;

B. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

C. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

D. An order instructing Francesca's to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

E. An order requiring Francesca's to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

F. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

G. An award of such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiffs demand a trial by jury on all triable issues.

DATED: February 8, 2024

Respectfully submitted,

*/s/ Jason S. Rathod*

Jason S. Rathod (*pro hac vice*)
Nicholas A. Migliaccio (*pro hac vice* anticipated)
**MIGLIACCIO & RATHOD LLP**
412 H St. NE, Ste. 302,
Washington, D.C. 20002
Tel: (202) 470-3520
Fax: (202) 800-2730
jrathod@classlawdc.com
nmigliaccio@classlawdc.com

Mason Barney (*pro hac vice*)
Tyler Bean (*pro hac vice*)
**SIRI & GLIMSTAD LLP**
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
mbarney@sirillp.com
tbean@sirillp.com

Nickolas J. Hagman (*pro hac vice*)
Daniel O. Herrera (*pro hac vice* to be filed)
Alexander J. Sweatman (*pro hac vice* to be filed)
**CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP**
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603

Telephone: (312)-782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com
asweatman@claffertyclobes.com

**COUNSEL FOR PLAINTIFFS AND THE PUTATIVE CLASS**

**CERTIFICATE OF SERVICE**

I hereby certify that a copy of the foregoing document was served on all counsel of record on February 8, 2024 via CM/ECF, in accordance with the Federal Rules of Civil Procedure.

*/s/ Jason S. Rathod*
Jason Rathod